

10.0 GENERAL

This chapter contains general information regarding escalating and resolving TSP System problems. The roles of the Manager, NCS and TSP Program Office, the National Coordinating Center (NCC), and the TSP Oversight Committee to assist with problem resolution are briefly discussed. TSP System audits are explained and service user recommendations regarding the TSP System are invited. Discussions of the international extension of the TSP System, preassigned priorities, preemption and security considerations are also in this chapter.

10.1 MANAGER, NCS AND TSP PROGRAM OFFICE

The Manager, NCS has been assigned the responsibility to administer the TSP System. In turn, the Manager, NCS has established a TSP Program Office to administer the TSP System on a day-to-day basis. In this capacity, the TSP Program Office assigns priorities within the TSP System and maintains information about TSP services in the NCS TSP data base. Service users should contact the TSP Program Office if they have any problems regarding the TSP System.

10.2 NATIONAL COORDINATING CENTER (NCC)

The NCC is a joint industry - government organization that is available to assist both government and the telecommunications industry in providing NSEP telecommunication services. It includes representatives from U.S. telecommunication industry corporations and Federal government agencies that are involved in responding to the Federal government's NSEP telecommunication service requirements. It also provides planning for a more enduring national and international telecommunications system to satisfy NSEP requirements. The NCC is resident within the NCS. (Contact the NCC for further information regarding the NCC's mission.)

For technical or procedural assistance in provisioning and/or restoring TSP services, a service user may seek assistance from the NCC. However, contact with the NCC is not intended to be the initial step for users to take in seeking assistance to provide or restore NSEP telecommunications service(s). Service users should first seek assistance through normal contacts within a service vendor organization before requesting the involvement of the NCC. NCC assistance should be sought only after alternative approaches have been explored and exhausted. (See Appendix E for contact information.)

10.3 TSP SYSTEM OVERSIGHT COMMITTEE

The TSP System Oversight Committee is responsible for identifying and reviewing any systemic problems developing in the TSP System. They are also charged with recommending

actions to correct or prevent recurrence of similar problems. In addition to representatives of the EOP, representatives from private industry (including telecommunication service vendors), state and local governments, the FCC, and other organizations may be appointed to this committee.

10.3.1 Purpose. The purpose of the TSP System Oversight Committee is to provide advice and assistance to the Manager, NCS in administering the TSP System and to ensure TSP System operational policies and procedures remain responsive to priority service requirements; and the TSP System remains current with telecommunications industry technical capabilities.

10.3.2 Responsibilities. The TSP System Oversight Committee provides a forum to facilitate identification, discussion, and resolution of systemic TSP System problems. The TSP System Oversight Committee is responsible for its internal organization, to include appointment of subcommittees and working groups.

10.4 AUDITS

A TSP audit is a quality assurance review conducted in response to identified problems. The purpose of an audit is to verify that established procedures and guidelines have been followed. An audit, as used here, is "procedural" as compared to "fiscal." The Manager, NCS is authorized to conduct audits as necessary. (As with other aspects of the TSP System, the Manager, NCS has assigned this responsibility to the TSP Program Office.) Any TSP service user, contracting activity, sponsor, or service vendor may request an audit and is required to cooperate during audits.

Before initiating an audit, the TSP Program Office will normally attempt to rectify systemic problems by meeting and discussing the issues with those experiencing the problem. Audits will be conducted only if other attempts to resolve a systemic problem have failed.

Before deciding to proceed with an audit, the TSP Program Office will review any documented evidence or records of TSP System procedural breakdowns. If the TSP Program Office decides to initiate an audit, written notification with appropriate information will be provided to the involved activities. The purpose of this written notification is to:

- Identify and describe the problem
- Indicate which activity reported the problem
- Solicit recommendations for solutions
- Indicate a reply date.

The involved activities will have 30 calendar days from the date of receipt of the audit notification to research their documentation relevant to the issue and to reply in writing. Activities that are unable to comply with this requirement must supply a written reply to the TSP Program Office, including a reason for the delay, as soon as they know they will not be able to meet the reply date. This reply must also include a proposed date for responding.

The TSP Program Office will submit results of the audit and recommendations to the TSP System Oversight Committee (see paragraph 10.3, TSP System Oversight Committee) for their evaluation, review, and comments. A TSP audit is not intended to replace the regulatory oversight role of the FCC, but rather to ensure the effective administration of the TSP System. Audits are intended to be used as a last resort, undertaken after all other attempts to resolve a problem have failed.

10.5 SERVICE USER RECOMMENDATIONS

The Manager, NCS is charged with reporting at least quarterly to the FCC and TSP System Oversight Committee the operational status of and trends in the TSP System, including:

- Numbers of requests processed and the priority levels assigned
- Relative percentages of services assigned to each priority level under each NSEP category and subcategory
- Any apparent serious misassignment or abuse of priority level assignments
- Any existing or developing problems.

The Manager, NCS will also include recommendations for action, as appropriate. Organizations participating in the TSP System are invited to submit recommendations or suggestions to the TSP Program Office for inclusion in this report. These recommendations or suggestions may include:

- How the TSP System is functioning, including problems experienced with the TSP System and their resolution
- What changes or improvements are required
- What technological advances have been developed or are anticipated that would improve the system's efficiency, cost effectiveness, or management structure

- What new services or capabilities should be included in the TSP System.

10.6 INTERNATIONAL EXTENSION OF THE TSP SYSTEM

Sometimes a service user requires an NSEP service that extends outside U.S. borders. It is desirable for priority treatment to be provided for all segments of that service. The TSP System, however, applies only to the U.S. portion of commercially provided, international telecommunication services. Service users may obtain TSP assignments for the U.S. portions of an international service, but they must make special arrangements to get priorities similar to TSP System priorities on the foreign portion of the service.

Service users obtain international services from U. S. international carriers. These carriers, in turn, negotiate with foreign governments or telecommunication companies (called their foreign correspondents) for international services. A U.S. international carrier's responsibility is for the link from the end user in the U.S. to a hypothetical midpoint. The foreign correspondent's responsibility is for the link from the hypothetical midpoint to the end user in the foreign country.

The foreign correspondent is responsible for their portion of the service, and a service user may arrange contractually for the U.S. international carrier to provide priority provisioning or restoration with the foreign correspondent under existing interoperating arrangements.

Some U.S. Government service requirements overseas are provided over facilities wholly owned by the U.S. Government. Agencies with such requirements should refer to their agencies' supplemental instructions for information on how to obtain priority treatment.

10.7 PREASSIGNED PRIORITIES

The TSP System allows the assignment of priority levels to any NSEP service across three time periods, or stress level conditions: Peacetime/Crisis/Mobilization, Attack/War, and Post-Attack/Recovery. Priority levels are normally assigned by the TSP Program Office and conveyed by the service user to service vendors only for the current time period. Priority levels may also be preassigned for the other two time periods at the request of service users who are able to identify and justify, in advance, their wartime or post-attack TSP service requirements. Priority assignments for other than the current time period are called preassigned priorities.

Industry capability does not currently support the ability to retain multiple priorities for a single service. Different priority levels required for a later time period must be changed by a service user submitting a "change" service order to the service vendor. It routinely takes 30 or more days for the change to take place.

To request a preassigned priority, a service user will submit a TSP Request (SF 315) to the TSP Program Office. The service user will indicate in TSP Request (SF 315) item 9, "Supplemental information," that the request is for a preassigned priority and provide a description of the event that must occur to trigger activation of this priority. (The TSP Request form is discussed in chapter 6.0. See paragraph 6.9 for specific information regarding item 9.)

The TSP Program Office will process requests for preassigned priorities upon receipt; however, a preassigned priority will not be authorized until the service user has notified the TSP Program Office that a previously described "event" has occurred. Once notified, the TSP Program Office will activate the preassigned priority by sending a TSP Authorization Code to the service user, and the service user will notify the service vendor, via a "change" service order, of the new priority assignment for that service.

The preassigned priority will be in effect until the service user notifies the TSP Program Office that the event that triggered the preassigned priority has ended, and the normal priority should be reinstated. After the TSP Program Office has been notified that the event has ended, the TSP Program Office will modify the priority assignment and will notify the service user. The service user, in turn, will notify the service vendor, via another "change" order, of the changed priority assignment.

Service users with requirements for preassigned priorities should discuss their requirements with the TSP Program Office prior to submitting a TSP request.

10.8 PREEMPTION

If suitable spare services are not available, service vendors are authorized to preempt existing services when necessary to provision or restore NSEP services. While preemption requires no action from service users, they should know what preemption entails. Preemption might be used to provision or restore one of their services; conversely, one of their services might be preempted to provision or restore another service user's TSP service.

Existing services without TSP assignments may be preempted to restore TSP services, or existing TSP services may be preempted to restore a TSP service with a higher priority level. When this is necessary, TSP services will be selected for preemption in the inverse order of priority level assignment. Service vendors who are preempting services will ensure their best effort to notify the user of the preempted service and state the reason for and estimated duration of the preemption. Preemption is a last resort for vendors, and service users should not expect it to occur routinely.

10.9 SECURITY CONSIDERATIONS

Classified information received by the TSP Program Office will be protected using measures appropriate to the classification level or sensitivity of the material. Access to classified information will be limited to appropriately cleared personnel. The message and mail addresses for transmitting classified information are in Appendix E.

The NCS TSP automated data base will be protected at the "Sensitive Information"¹ level. Access to the NCS TSP data base will be limited to U.S. Government employees and contract employees (U.S. citizens) that have a need to access the data base to perform their jobs. All communications links for the TSP computer facility will be encrypted. No classified information will be placed in the NCS TSP data base.

TSP Request forms (SF 315) and TSP Invocation Reports (SF 320) may be handled through special procedures by prearrangement with the TSP Program Office in order to protect classified and/or sensitive information. Classified TSP Request forms (SF 315) and TSP Invocation Reports (SF 320) must be appropriately marked by the service user and sent through proper channels.

¹ The term "sensitive information" means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled ... but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (From P.L. 100-235, Jan. 8, 1988)